Homework #8 Solutions

4.4.1. (a) We find the roots of $f(X) = X^2 + 4X + 2$ modulo 7 by brute force:

$$\begin{aligned}
0^2 + 4 \cdot 0 + 2 &= 2 \not\equiv 0 \pmod 7 \\
1^2 + 4 \cdot 1 + 2 &= 7 \equiv 0 \pmod 7 \\
2^2 + 4 \cdot 2 + 2 &= 14 \equiv 0 \pmod 7 \\
3^2 + 4 \cdot 3 + 2 &= 23 \equiv 2 \not\equiv 0 \pmod 7 \\
4^2 + 4 \cdot 4 + 2 &= 34 \equiv 6 \not\equiv 0 \pmod 7 \\
5^2 + 4 \cdot 5 + 2 &= 47 \equiv 5 \not\equiv 0 \pmod 7 \\
6^2 + 4 \cdot 6 + 2 &= 62 \equiv 6 \not\equiv 0 \pmod 7.
\end{aligned}$$

So the roots are given by $x \equiv 1, 2 \pmod 7$.
(b) Hensel's lemma tells us exactly how to lift each of the two incongruent roots modulo 7 to roots modulo $49 = 7^2$. We need the formal derivative $f'(X) = 2X + 4$. First consider $x \equiv 1 \pmod 7$. Since $f'(1) = 2 + 4 = 6 \not\equiv 0 \pmod 7$, Hensel's lemma implies that 1 lifts uniquely to a root modulo 49 given by $x_2 \equiv 1 + 7t \pmod{49}$, where $t \equiv -\overline{f'(1)}(f(1)/7) \pmod 7$. By inspection, we can take $\overline{f'(1)} = 6$, so

$$t \equiv -\overline{f'(1)}\frac{f(1)}{7} \equiv -6\frac{7}{7} = -6 \equiv 1 \pmod 7.$$

Thus the unique lift of 1 to a root modulo 49 is given by $x_2 \equiv 1 + 7 = 8 \pmod{49}$. Now we consider the root $x \equiv 2 \pmod 7$. Since $f'(2) = 2 \cdot 2 + 4 = 8 \equiv 1 \not\equiv 0 \pmod 7$, once again Hensel's lemma implies that there is a unique lift to a root modulo 49 given by $x_2 \equiv -f'(2)(f(2)/7) \pmod{49}$, where $t \equiv -\overline{f'(2)}(f(2)/7) \pmod 7$. We can take $\overline{f'(2)} = 1$, so

$$t \equiv -\overline{f'(2)}\frac{f(2)}{7} \equiv -1\frac{14}{7} \equiv -2 \equiv 5 \pmod 7.$$

Thus the unique lift of 2 to a root modulo 49 is given by $x_2 \equiv 2 + 7 \cdot 5 \equiv 37 \pmod{49}$. Summarizing, the roots modulo 49 are given by $x_2 \equiv 8, 37 \pmod{49}$.

6.1.18. We have $24 = 3 \cdot 8$, and since $(3, 8) = 1$, it suffices to show that $n^2 \equiv 1 \pmod 3$ and that $n^2 \equiv 1 \pmod 8$. First, since 3 does not divide n, $(3, n) = 1$, and Fermat's little theorem implies that $n^2 \equiv 1 \pmod 3$. Now, as n is odd, we may write $n = 2k + 1$ for some integer k. We then have $n^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$. At least one of $k, k + 1$ is even, so $4k(k + 1)$ is a multiple of 8, and therefore $n^2 = 4k(k + 1) + 1 \equiv 1 \pmod 8$. We may now conclude that $n^2 \equiv 1 \pmod{24}$.

6.1.19. We have $35 = 5 \cdot 7$, so, since $(5, 7) = 1$, it suffices to show that $a^{12} - 1$ is divisible by both 5 and 7. As $(a, 35) = 1$, we also have $(a, 5) = 1 = (a, 7)$, and it follows from Fermat's little theorem that $a^4 \equiv 1 \pmod 5$ and that $a^6 \equiv 1 \pmod 7$. Cubing both sides of the first

Date: April 5, 2018.

congruence gives $a^{12} \equiv 1 \pmod 5$, and squaring both sides of the second congruence gives $a^{12} \equiv 1 \pmod 7$. Thus $a^{12} - 1$ is divisible by both 5 and 7, and hence by 35.

6.1.24. By Theorem 6.4, for any integer a, $a^p \equiv a \pmod p$. Therefore

$$1^p + 2^p + \cdots + (p-1)^p \equiv 1 + 2 + \cdots + (p-1) \pmod p.$$

We have $\sum_{j=1}^{p-1} j = ((p-1)/2)p$, and because p is odd, 2 divides $p-1$, so p divides $\sum_{j=1}^{p-1} j$, i.e.,

$$1 + 2 + \cdots + (p-1) \equiv 0 \pmod p.$$

6.1.29. By Wilson's theorem, $(p-1)! \equiv -1 \pmod p$, so, on multiplying both sides of this congruence by $-a$, we find that $-(p-1)!a \equiv a \pmod p$. Moreover, Theorem 6.4 implies that $a \equiv a^p \pmod p$. Combining the last two congruences gives $-(p-1)!a \equiv a^p \pmod p$, which means that p divides $a^p - (-(p-1)!a) = a^p + (p-1)!a$.

6.1.42. For the record, the binomial theorem says that, for real numbers x and y and a positive integer n, $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$. We therefore have

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k.$$

Since p divides $\binom{p}{k}$ for $1 \le k \le p-1$, the sum in the final expression of the displayed equation is divisible by p, so, on reducing modulo p, we obtain $(a+b)^p \equiv a^p + b^p \pmod p$. This congruence is known as the Freshman's Dream.

6.3.3. If $m = 1$, then $a \equiv b \pmod m$ for all integers a and b, so there is nothing to show. We will therefore assume that $m > 2$. For any integer a, $(a, m) = (-a, m)$, so if a is relatively prime to m, then $-a$ is as well. Moreover, if $a \equiv -a \pmod m$, then m divides $2a$. Since $m > 2$, either m is divisible by an odd prime p, and p necessarily also divides a, or m is divisible by 4, which implies that 2 divides a. In any case $(a, m) \neq 1$, so if a is relatively prime to m, then a cannot be its own additive inverse modulo m. Combining these observations, we see that the integers $c_1, \ldots, c_{\varphi(m)}$ can be put into pairs consisting of additive inverses modulo m. Therefore the terms of the sum $c_1 + \cdots + c_{\varphi(m)}$ may be grouped according to this pairing, from which it follows that $c_1 + \cdots + c_{\varphi(m)} \equiv 0 \pmod m$.

6.3.10. Since $(a, b) = 1$, applying Euler's theorem with modulus b gives $a^{\varphi(b)} \equiv 1 \pmod b$. On the other hand, we certainly have $b^{\varphi(a)} \equiv 0 \pmod b$. Adding these congruences gives $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod b$. By symmetry, we also have $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod a$. Using once more that a and b are relatively prime, we may conclude that $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$.